Cyber Security - Michigan's Critical Infrastructure

Presentation to the Michigan Senate Energy & Technology Committee

Patrick Hudson and Alex Morese

Michigan Public Service Commission

12/10/13

Role of MPSC

Assure the security of the State's critical infrastructure by promoting homeland security.

MPSC Mission Statement

The MPSC is the primary state liaison to energy and telecommunications companies with regard to service disruptions and restoration, system damage, and impacts affecting (or potentially affecting) incident response and recovery and emergency services.
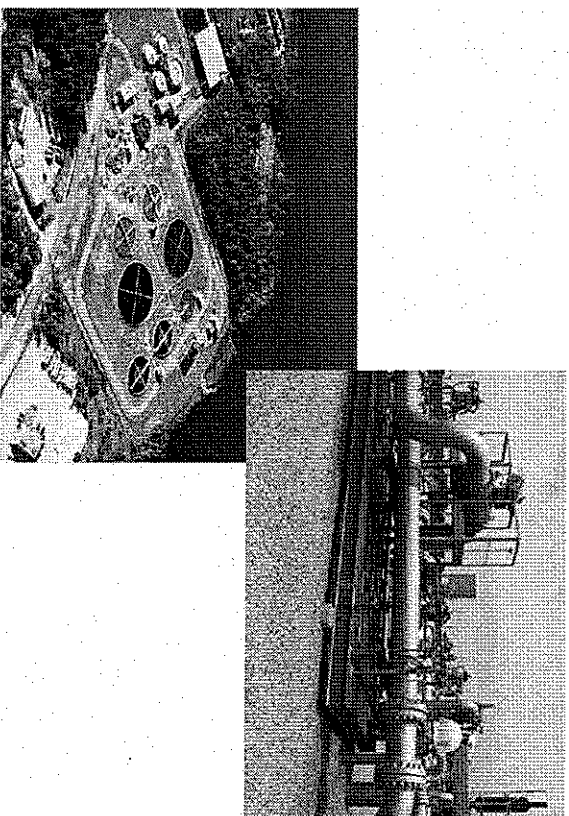
MICHIGAN PUBLIC SERVICE COMMISSION

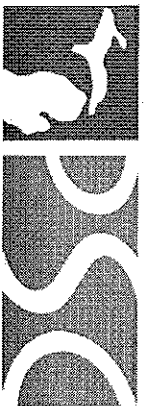Michigan Emergency Management Plan (MEMP)

Critical Infrastructure: Utility Sectors

- Electricity
- Natural Gas
- Telecommunications
- Petroleum

- *Includes: physical infrastructure, electronic equipment, communication systems, and data.*
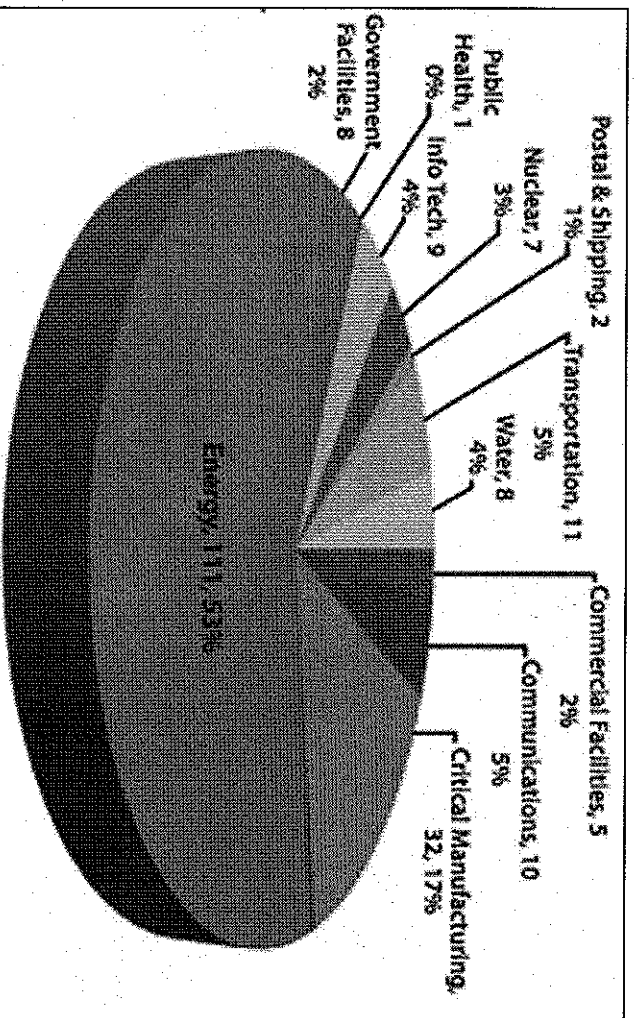
Cyber Attacks on Utility Sector

The Energy Sector accounted for 53% of all cyber incidents reported to DHS in the six months ending in May 2013.

Postal & Shipping, 2
1%

Nuclear, 7
3%

Public
Health, 1
0%

Info Tech, 9
4%

Government
Facilities, 8
2%

Transportation, 11
5%

Water, 8
4%

Energy, 111, 53%

Commercial Facilities, 5
2%

Communications, 10
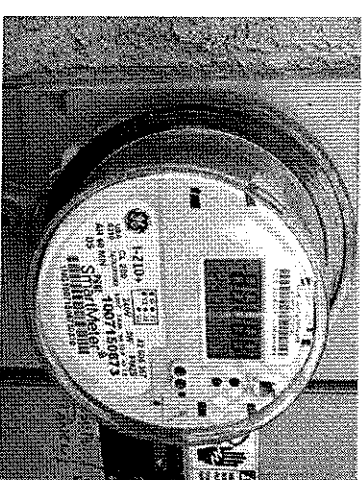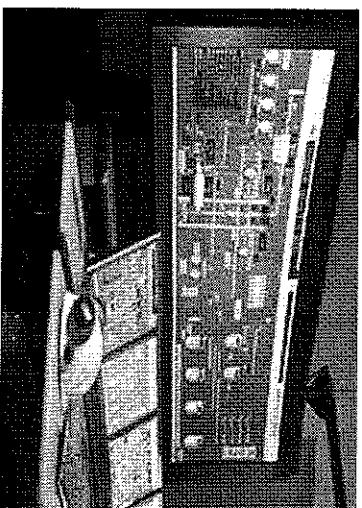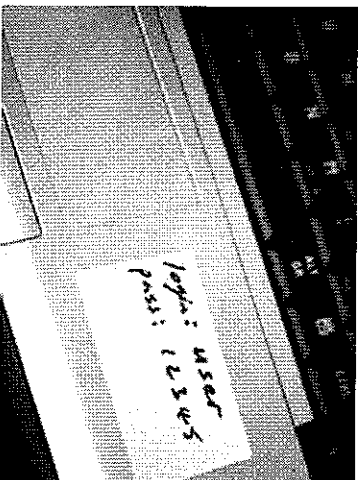5%

Critical Manufacturing,
32, 17%

More than 200 incidents from Oct. 2012 – May 2013.

MICHIGAN PUBLIC SERVICE COMMISSION

Utility Cyber Security Targets

- Information Technology Systems
- Supervisory Control and Data Acquisition Systems (SCADA)
- Smart Grid
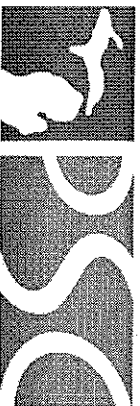
Historical Cyber Events at Utilities

August 15, 2012
Saudi Aramco – Saudi Arabia
- Attempt to disrupt flow of oil and gas
- Supplies 10 percent of world oil
- Damaged about 30,000 computers
- Hacker group claimed responsibility; national backing suspected.
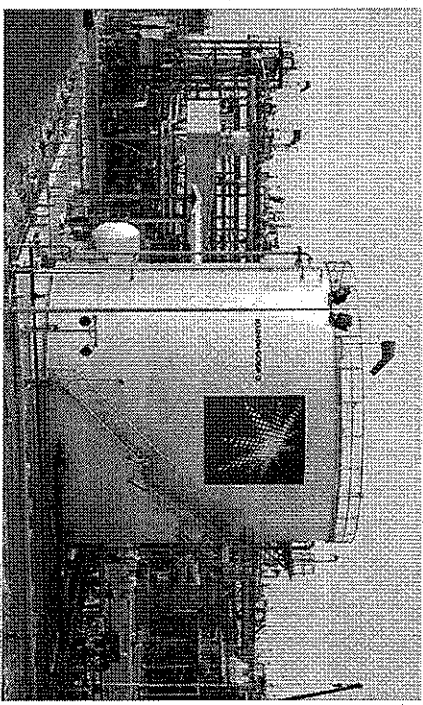
November, 2012
SCADA Honey Pot – United States
- Virtual water company
- Diversionary ICS/SCADA system
- First attack within 18 hours
- After 28 days, 39 attacks from 14 countries

Cyber Security: the National Front

- Executive Office
- Congress
- Department of Homeland Security
- Department of Energy
- Federal Communications Commission (FCC)
- Federal Energy Regulatory Commission (FERC)
- North American Electric Reliability Corporation (NERC)
- National Institute of Standards and Technology (NIST)
- National Electric Sector Cybersecurity Organization (NESCO)

Federal Emphasis: Electricity Sector

NERC CIP Reliability Standards – Bulk Transmission System

- Identify Critical Cyber Assets (CCAs) and authorized users
- Implement cyber & physical protective measures of CCAs
- Training on security policies and awareness
- Incident response
- Backup and recovery
- 8 Standards/43 High-Level Requirements/168 Total Requirements

PSC
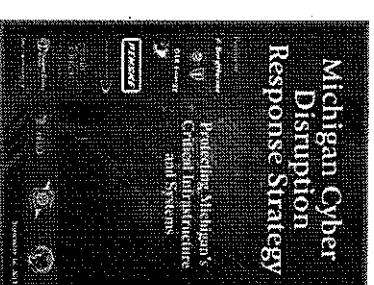
MICHIGAN PUBLIC SERVICE COMMISSION

State Emphasis: Cyber Disruption Response Strategy

Strategic Goals

- Improve situational awareness among CI owners and operators.
- Create operational plans for response to and recovery from cyber disruption events.
- Train key staff; exercise communication and response plans.
- Conduct risk assessments to identify vulnerabilities of Michigan's CI.

Recent Activities

- Executive Cyber Tabletop Exercise (Lansing – Oct. 1)
- Michigan Cyber Summit (Novi – Oct. 25)

Michigan Cyber Disruption Response Strategy

Protecting Michigan's Critical Infrastructure and Systems

MPSC Emphasis: Smart Grid Staff Report

U-17000, June 2012

Addressed deployment, safety and other issues related to smart meters, including cyber security.

- Staff cyber security recommendations:
  - Annual independent security audits
  - Maintain a dialogue with utilities re: standards compliance and preparedness measures
  - Uniform breach notification strategy
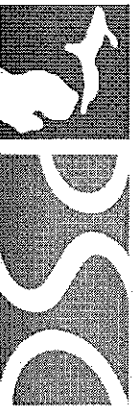
MICHIGAN PUBLIC SERVICE COMMISSION

MPSC Approach

1. Remain knowledgeable of cyber security issues and threats

   - Cyber security standards and guidelines
   - Training and exercises

2. Assess the status of cyber security and smart grid developments

   - Role of "monitoring" and "cognition" of cyber security practices
   - Emphasize the accountability of the "process" rather than full disclosure of the "details"

3. Strengthen public and private partnerships

   - Encourage data, threat and information sharing

MICHIGAN PUBLIC SERVICE COMMISSION

1. Cyber Security Issues and Threats

Best Practices

- Cyber security efforts should concentrate on rigorous open standards and guidelines through public-private partnerships

- Effective Cyber Security will rely on data sharing and cooperation between regulatory, private and industry entities.

- A risk-based approach to cyber security planning should be implemented.

- Regulatory bodies should be in constant contact with asset owners regarding cyber security.

MICHIGAN PUBLIC SERVICE COMMISSION

2. Cyber Security Assessments
Utility Cyber Plans

- Briefings have been presented to the MPSC by:
  - AT&T
  - Comcast
  - Consumers Energy
  - DTE Energy
  - International Transmission Corporation (ITC)
  - National Association for Regulatory Utility Commissioners (NARUC)
  - Reliability First (Regulation Entity for NERC)
  - TransCanada

3. Public/Private Partnerships
MI Utility Cyber Security Forum

- Initial dialogue about cyber security with Michigan energy providers and other stakeholders
  - Investor Owned, Municipal, and Cooperative Utilities; Transmission Companies
  - State of Michigan: MPSC & DTMB
  - Discussed views of top threats, cyber security strategies, best practices, communication strategies
- Phase one of a continued dialogue & networking process

MICHIGAN PUBLIC SERVICE COMMISSION

Next Steps

- Utility Cyber Security Forum (voluntary)
  - Extend invitations to include telecommunications, water, and petroleum critical infrastructure providers.
  - Establish a collaborative format for discussion, relationship building, resources sharing, and best practices development for all stakeholders.

- U-17000
  - Develop cyber security policy for MPSC

Thanks for your attention.

Alex Morese **Energy Data and Security** **517-241-0292** **moresea@michigan.gov**	**Patrick Hudson** **Smart Grid** **517-241-9452** **hudsonp1@michigan.gov**